qll

UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/827,226	04/05/2001	Marcus Wong	1	6211

7590   05/11/2007

David J. Gaskey
Carison, Gaskey & Olds, PC
400 West Maple Road
Suite #350
Birmingham, MI 48009

EXAMINER
SHIFERAW, ELENI A

ART UNIT	PAPER NUMBER
2136	

MAIL DATE	DELIVERY MODE
05/11/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

PTOL-90A (Rev. 04/07)

MAILED

MAY 11 2007

Technology Center 2100

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 09/827,226
Filing Date: April 05, 2001
Appellant(s): WONG, MARCUS

David J. Gaskey
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 01/08/2007 appealing from the Office action mailed

10/23/2006.

1.   ***Real Party Interest***
      A statement identifying the real party in interest is contained in the brief.

2.   ***Related Appeals and Interferences***

      The brief does not contain a statement identifying the related appeals and interferences

      which will directly affect or be directly affected by or have a bearing on the decision in

      the pending appeal is contained in the brief. Therefore, it is presumed that there are none.

      The Board, however, may exercise its discretion to require an explicit statement as to the

      existence of any related appeals and interferences.

3.   ***Status of the Claims***
      The statement of the status of the claims contained in the brief is correct.

4.   ***Status of Amendments After Final***
      The Appellant's statement of the status of amendments contained in the brief is correct.

5.   ***Summary of Claimed Subject Matter***
      The summary of claimed subject matter contained in the brief is correct.

6.   ***Ground of Rejection to be Reviewed on Appeal***
      The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

7.   ***Claims Appendix***
      The copy of the appealed claims contained in the Appendix to the brief is correct.

8.   Evidence Relied Upon

"Dynamic Participation in a Secure Conference Scheme for Mobile Communications"	Min-Shiang Hwang herein after "the Hwang '99 reference"	09-1999

9.   ***Ground of Rejection***
      The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 102

1.   The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the

basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

2.   Claims 21-40 are rejected under 35 U.S.C. 102(b) as being anticipated by Hwang (IEEE

'99, Dynamic Participation in a Secure Conference Scheme for Mobile communications).

Regarding claims 21 and 33 Hwang discloses a method of providing secure communications

between a first wireless unit that uses a first session key and a second wireless unit that uses a

second session key, the method comprising:

generating a common key value as a function of at least a portion of at least one of first

session key or the second session key (page 1470 section II A steps 1 and 4; *random number r11*

and r12 is a session key-decryption key);

providing/receiving the common key value to the first wireless unit (page 1471 col. 1

lines 17-24; *trusted network center (NC) generating and providing common key to the first*

wireless terminal (T1)) for use in secure communications between the first wireless unit and the

second wireless unit having the common key value (page 1471 col. 1 lines 19-20 and page 1469

section I paragraph 3; *any participant (second or third terminals) gets common key, for secure*

*mobile communications **without the communication unit involving to encrypt/decrypt message***

exchanged between the terminals).

Regarding claim 22, Hwang discloses the method comprising:

sending the common key value to the first wireless unit using the first session key (see,

fig. 1 element g; *common key is sent to Ti that is generated based on **terminal 1** => r11 and r12*

session key-decryption key).

Regarding claim 23, Hwang teaches the method comprising

sending the common key value to the second wireless unit using the second session key

(see, fig. 1 element g; *common key is sent to Ti that is generated based on **terminal 2** => r11*

and r12 session key-decryption key).

Regarding claim 24, Hwang discloses the method comprising

encrypting the common key value with the second session key (page 1470 steps 7-9;

common key is encrypted using NC's key); and

transmitting the encrypted common key value to the second wireless unit (page 1470-

1471 section II; *encrypted CK is transmitted to Ti*).

Regarding claim 25, Hwang teaches the method comprising

encrypting the common key value using the first session key (page 1470 steps 7-9;

common key is encrypted using NC's key according to next terminal); and

transmitting the encrypted common key value to the first wireless unit (page 1470 steps

7-9; *transmitting encrypted common key to Ti*).

Regarding claim 26, Hwang discloses the method comprising

generating the first session key as a function of a first root key known only at the first wireless unit and a wireless communication system accessed by at least the first wireless unit (see page 1470 section II A step 4; *each terminal generating random number as a session key-decryption key*).

Regarding claim 27, Hwang discloses the method comprising

generating the second session key as a function of a second root key known only at said second wireless unit and at a home wireless communication system accessed by at least said second wireless unit (page 1470 section A steps 1-7; *Network center generating common secret session key CK for each participant terminals based on random number each terminal generate*).

Regarding claims 28 and 39, Hwang discloses the method comprising

generating the common key value as a function of the first session key and the second session key (page 1470 section A steps 1-7; *Network center generating common secret session key CK for each participant terminals based on session key-decryption key*).

Regarding claim 29, Hwang discloses the method comprising

generating the common key value as an encryption key (abstract; *CK for encryption*).

Regarding claim 30, Hwang teaches the method comprising

generating the common key value as a session key (page 1471 lines 19-20; *CK, common secret session key*).

Regarding claim 31, the method comprising

mutually generating the common key value by a first wireless communicating system

accessed by the first wireless unit and a second wireless communication system accessed by the

second wireless unit (page 1470 fig. 1).

Regarding claims 32 and 40, Hwang teaches the method comprising

using the common key value for a first communication session between the first and

second wireless units (pages 1470-1471 section I); and

using the same communication key value for a second, different communication session

between the first and second wireless units (pages 1470-1471 section I).

Regarding claim 34, Hwang teaches the method comprising

generating the first session key corresponding to the first wireless unit (page 1470 section

II; *terminal-1 with key e (AK1) (r11 and r12 session key-decryption key) ...that is used to request*

*session key from network center, and **Applicant Admitted Prior Art (AAPA) explains root***

key/A_key/AK1, on page 3-5, as a well-known); and

obtaining the common key value by the first wireless unit using the first session key

(Hwang page 1470 steps 7-9; $CK=(Q.2^2 + R) \ mod \ ri$).

Regarding claim 35, Hwang discloses the method comprising

decrypting the common key value using the first session key (page 1470 steps 4-7).

Regarding claim 36, Hwang discloses the method wherein

the first session key is generated as a function of a first root key known only at the first

wireless unit and a wireless communication system accessed by at least the first wireless unit

(page 1470 section A steps 1-7; *Network center generating common secret session key CK for*

each participant terminals based on random number each terminal generate).

Regarding claim 37, Hwang discloses the method comprising

using the common key as an encryption key (abstract; *CK for encryption*).

Regarding claim 38, Hwang discloses the method comprising

using the common key as a session key (page 1471lines 19-20; *CK, common secret*

session key).

3.   Claims 21 and 33 are also rejected under 35 U.S.C. 102(b) as being anticipated by Hwang

'92, (IEEE 1992, Scheme for secure digital mobile communications based on symmetric key

Cryptography).

Regarding claims 21 and 33, Hwang '92 discloses a method of providing secure communications

between a first wireless unit and a second wireless unit that uses a second session key, said

method comprising the step of:

generating a common key value as a function of at least a portion of at least one of the

first session key or the second session key and receiving at the first wireless unit, a common key

value (page 423 section II; *generating a common key based on nonce*); and

providing a common key value to a first wireless unit for use in secure communications

over at least one wireless communications system between said first wireless unit and said

second wireless unit having said common key (page 423 section II; *network center provides*

session symmetric key & nonce to the mobile unit-1...mobile unit-1 decrypts the encrypted

session symmetric key & nonce and compares the nonce unit-1 sent with received and if

match, unit-1 encrypts the message using symmetric session key and sends the encrypted

message & unit-2 nonce to mobile user-2.... unit-2 authenticates the nonce same as unit-1 and

decrypts the encrypted message sent from user-1 using symmetric session key and mobile unit-

1 and unit-2 are securely communicated without the network center encrypting and decrypting

messages exchanged between the units and/or no significant amount of processing by the

network center is required to encrypt/decrypt data sent between the first and second mobile

units).

10.   *Response to Argument*

The Hwang '99 reference does anticipate Claims 21-40.

The appellant's first argument concerns with the Hwang '99 reference failure to

disclose generating a common key as a function of at least a portion of a session key associated

with a wireless unit as disclosed on page 4 paragraph 2-4 of the Appeal Brief. The examiner

respectfully disagrees with the appellant's contentions and would like to draw the Appellant's

attention to page 1470 section II-page 1471 col. 1 lines 24 wherein Hwang '99 reference

discloses the Network Center (NC) generating a common key (CK) and providing CK to users

Ui of wireless terminals Ti, and the NC generating CK by receiving random numbers rl=rl1+rl2

and/or ri1 and ri2 as **a session key-decryption key** from the wireless terminals (see step 1 and

step 4). **As applicant agreed on page 4 lines 16-17 of the brief, ri being a session key-decryption key used by each terminals the ri is not just random numbers but session key-decryption key.** NC generating CK from r0, r1, ..., rm (ri) session key-decryption key (see step

9). Since CK is generated from ri session key-decryption key, CK is a function of session key.

The random numbers used to generate the CK are not just random numbers as the appellant

argues, the reference clearly states that the random number being a session key-decryption key

(see step 1 and 4).

The appellant's second argument concerns with the Hwang '99 reference not disclosing a

common key value that is a function of at least a portion of a session key associated with a

wireless unit as disclosed on page 4. Argument is not persuasive because a common key value

(CK of the Hwang '99 reference) is generated from ri session key-decryption key of the T1 (see

steps 1-9). Terminals Ti transmitting ri session key-decryption key to NC and NC generating CK

from ri session key-decryption of terminals and/or CK = (CK + lcm(**r0, r1, ..., rm**) mod **ri.**

Therefore CK is a function of ri(session key).

The examiner disagrees with the appellant's unfinished sentence citation on the

appellant's brief argument page 4 lines 17-18 wherein "...and CK to indicate a common secret

session key of a secure teleconference that is chosen randomly by the NC. The examiner would

like to correct the appellant because the CK is not only chosen randomly by NC **but also ri1 and

ri2** (see the Hwang '99 reference col. 1 lines 18-20) Hwang '99 reference discloses "... CK be a

common secret session key of length 255 b of the secure teleconference chosen randomly by **NC,**

ri1, and ri2…" and also in steps 7-9 of Hwang '99 reference states that NC choosing nonzero

random numbers CK and r0 to generate CK that is (CK + lcm(r0, r2, …, rm) mod ri wherein ri is

a session key-decryption key. Therefore CK is a function of session key.

The appellant's next argument concerns with Hwang reference '99 on page 1471

indicating that the NC choosing non zero random numbers CK and the random numbers not

being a function of any portion of the session keys (brief page 5 par. 1). Argument is not

persuasive because NC chooses nonzero random numbers CK and r0, and computes CK+lcm(r0,

r1, …, rm) (see steps 7-9), and Ti receives $CK=((Q(2^y)) + R) \bmod ri)$ wherein $((Q(2^y)) + R)$ is

PI = (CK + lcm(r0, r2, …, rm) and generates CK that is ((CK + lcm(r0, r2, …, rm) mod ri);

wherein ri is session key-decryption key of Ti (see steps 1 and 4). Since CK is generated for ri.

CK is a function of session key.

Therefore the Hwang reference does anticipate all claims 21-40.

<u>The Hwang '92 reference not anticipating either of claims 21 or 33</u>

The examiner withdraws the rejection to claims 21 or 33 based on Hwang '92 but

maintains the rejection 21-40 based on Hwang '99.

11.   ***Related Proceeding(s)***
        No decision rendered by a court or the Board is identified by the examiner in the Related
Appeals and Interferences section of the examiner's answer.

12.   ***Conclusion***
        For the above reasons, it is believed that the rejections should be sustained.

        Respectfully submitted,
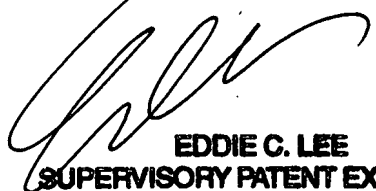
May 2, 2007
Conferees:
Arani Taghi

Eddie Lee

EDDIE C. LEE
SUPERVISORY PATENT EXAMINER

Eleni Shiferaw